Securing Electronic Government

January 19, 2001

Prepared by

Security, Privacy, and Critical Infrastructure Committee

Background

On May 31st 2000, representatives from Government and industry met to begin a discussion on security benchmarks Federal agencies can use as points of departure when implementing electronic government (e-gov) services. The meeting, sponsored by the CIO Council, the CFO Council, and the Information Technology Association of America (ITAA), was just the first in what may become a series of discussions between Government and industry to develop a resource guide for Chief Information Officers (CIOs) as they champion e-gov initiatives within their departments and agencies. This document represents a summary of the proceeding of the May 31st, 2000 meeting, with additional case study materials added, to be used for discussion purposes and does not represent government policy or specific recommendations on the part of the sponsoring organizations. Rather, this document is intended to increase the recognition of specific security issues and lead to further discussion in the area of improving security related to implementing electronic government services.

Purpose

The purpose of this document is to discuss security in the context of three e-government services: web-based information services, Government and industry procurement, and financial transactions to the public. Many times risk assessments provide a wide range of options; knowing what is right for a particular e-gov service is not always obvious. This document seeks to answer the following questions when presented with a wide range of choices:

- How does the type of electronic transaction affect security priorities and solutions?
- How might one decide where along the security continuum one should land?
- What are some practical ways one might go about determining whether the selected security measures are sufficient?

Document Overview

This introductory section presents an overview of some challenges faced by the Government community in e-gov security. These challenges, many times, will drive the Government to a more stringent security solution than might be undertaken in the commercial world. The sections that follow present example solution sets for a given e-gov service. Each part discusses why an organization might choose two different security solutions, even when offering the same e-gov service. The discussion is organized around five security goals: availability, authentication and identification, confidentiality, integrity, and non-repudiation. They are defined as follows:

- **Availability**—Timely, reliable access to data and services for authorized users. This includes the restoration of services after an interruption.
- **Identification and Authentication**—Identification is the process an information system uses to recognize an entity. Authentication establishes the validity of a transmission, message, or originator, and verifies authorization for the user to receive specific categories of information.

- **Confidentiality**—Assurance that information is not disclosed to unauthorized persons, processes, or devices.
- **Integrity**—Protection against unauthorized modification or destruction of information.
- **Non-repudiation**—Provides the sender with proof of delivery and the recipient with proof of the sender's identity, so neither can later deny having processed the data.

Many of the solutions in each goal area address strategic or policy-oriented considerations. The first step in many cases entails making decisions on issues such as the importance of the information, who should have access, and whether legal challenges may arise in the wake of a security incident. As demonstrated in the following sections and case studies, the importance of each goal varies according to the answers to these questions; answers which may drive decision-makers to look at alternative technical and policy solution.

This document is not a complete guide to e-gov security. Rather, it is simply the beginning of an evolving conversation in this area. It is also not intended to be a source of technical information; documents like the Information Assurance Technical Framework and standards such as the Common Criteria can provide specific technical solutions and product recommendations. Similarly, methodologies presented in the three case studies are illustrative examples of how organizations considered security goals and solutions in light of the particular type of electronic service they provide. They are not endorsements of a particular approach, nor do they reproach solutions that the organization did not select.

Summary Organizational Challenges

E-gov today involves the exchange vital and often sensitive information. Millions of dollars—as well as public confidence—are at stake. In this environment, brimming with opportunity, challenges are numerous. For the purposes of this document, the challenges are grouped into three categories: Government and private sector differences, legal landscape issues, and organizational concerns.

The Government is often held to higher standard than the private sector. Areas in which this difference is manifest include:

- High public expectations; glitches, down time are unacceptable.
- The Government's need to balance providing a service that is easy to use and ensuring that it maintains confidentiality and integrity.
- User desire for a single portal for all their interactions with the Government, but without Government organizations sharing data with one another.
- User willingness to accept some risk when doing business with the private sector, in contrast to their desire for total security when interacting with the Government.

- Greater risks if Government-held information is released (it affects one's ability to get important government services like Social Security and Medicare), versus somewhat lesser risks in the private sector (for example, credit card liability is only $50).

The second category of challenges the legal landscape:

- Standards for authentication and non-repudiation may be higher in the digital environment. In paper world a wet ink signature required no additional verification. In contrast, digital signatures are often required for authentication in online environment.
- The legal and regulatory landscape may not have caught up to the changes brought on by the e-commerce environment.

The third category of challenges is organizational:

- Many departments and agencies face internal resistance when implementing e-gov services. Employees may view this evolution as a threat to their jobs.
- Senior managers may not understand the security challenges or be willing to commit sufficient resources.
- Even when the need for security is recognized, resources may not be available (either skilled staff or dollars).

These challenges are applicable to all three categories of e-gov services discussed below.

SECURING ELECTRONIC GOVERNMENT
WEB-BASED INFORMATION SERVICES

Chairs: Dave Nelson, Deputy CIO, NASA
Bill Marlow, Global Integrity

BACKGROUND

Some of the most pervasive e-gov services are those that offer web-based information to the public. These services range from simply providing basic information on times of operation and locations of Government offices to public service information on important topics such as tax regulations and medical developments. Government agencies are also offering forms on line for federal and state taxes, social security cards, driver's licenses, passports, etc.

Because the Government's "customers" comprise the population of the United Sates and, in some cases, the world, most of its web sites allow unrestricted access. In general, users of the web site are not required to enter any information to gain entry to the site. Of the three types of e-gov services, therefore, web-based information is the most widely accessible.

The public nature of the information and the web sites' wide accessibility may cause organizations to consider security unimportant. After all, who would want to steal what is free? Indeed, until recently those working on openly available web-based information services paid very little attention to the security goals of confidentiality, integrity, availability, authentication, and non-repudiation.

Two developments have changed this attitude. First, the public increasingly relies on Government web sites for reliable information. The effect is that organizations need to ensure that their information is not only available, but also correct. Second, the number and impact of "unfortunate events" has intensified. These can range from "acts of God," such as power outages due to storms, to attacks from insiders or outsiders bent on changing the content of the information, defacing a web site to protest a Government policy, or overloading the web site with spurious requests to deny service to users.

Government organizations are beginning to recognize the importance of including security considerations in up front planning for web-based information services. One cannot simply make a priori decision about security requirements; each service should be examined on an individual basis. The most important first step is to create a security plan. The purpose of the plan is to analyze what can go wrong and to determine responses that reduce the likelihood and consequences to an acceptable level. The discussion below illustrates how security considerations vary with the nature of the web site.

IMPLEMENTING SECURITY

The two minimum essential security goals in this area are **availability** and **integrity**. As mentioned in the introductory section, Government is often held to a higher standard than industry. The same consumer may find it acceptable for a store's web site to be unavailable, but unacceptable for a Government web site to be unavailable since there are no alternatives. In the most extreme cases, public confidence in Government could be adversely affected by disruptions in web-based information services.

Building on availability, the next minimum essential security requirement is integrity. Of course every organization wants to ensure their information is correct. However, in some cases organizations will not want to expend scarce resources to ensure data integrity. In other cases, of course, the cost of incorrect information may be greater than the preventive measures. For example, a library may have its holdings listed on line. If the list is altered, the cost may only be inconvenience to the public and would not merit any action more sophisticated than a periodic visual or automated check. However, in the case of medical information that affects citizen's health or welfare, incorrect information could be a life-and-death matter and more stringent measures would be warranted. Another, less obvious case might be hours of operation for a key Government office. Techniques are available to ensure the information has not been altered. These include off-line copies of the information that are compared periodically with the on-line information and digital signature algorithms that determine whether the data has been altered.

Confidentiality is becoming an increasingly significant issue for Government web-based information services. In this context, meeting the goal of confidentiality entails ensuring that any information collected from the public in the course of a web site visit is kept confidential. One situation where this security goal may be important is the case of medical information. For example, researchers may not mind if they are observed gathering data from a disease information web site. However, individuals with the disease may be very interested in ensuring their anonymity.

Web technology allows organizations to track the activities of users over time through the use of "cookies." Cookies are small text files sent by a web site to a user's browser and stored on the user's computer. They contain information about sites the user has visited and can be queried to reveal information about the user's web activities. It is important to ensure that organizations publicize clear policies about what information they collect. OMB has excellent suggestions for privacy policy statements that organizations can post on their web sites.[1] Moreover, recent breaches of confidentiality by Government organizations has led OMB to issue a memo precluding Government web sites from using cookies unless they meet very specific conditions.[2] In fact, a description of each organization's practices in this area is now required in its budget submission.

---

1 *See http://plainlanguage.gov/example/other/privacy%20policy.htm*

2 *OMB-M0013, Memorandum for the Heads of Executive Departments and Agencies, June 22, 2000.*

Non-repudiation is an emerging security goal. As with integrity, the importance of non-repudiation grows with the impact on the citizen. Consider the case in which tax guidelines are provided to, and subsequently acted upon by a citizen. In this hypothetical case, the citizen is assessed a stiff penalty for having submitted incorrect financial data. The citizen then claims that he or she is not responsible for the penalty, having not received the information from the Government agency. To protect itself, it would be beneficial in this instance for the Government organization to provide proof that the information was delivered.

Finally, ensuring **identification and authentication** is required for agencies providing individualized web-based information such as tax or health records, on-line voting, etc. In these cases, particular attention must be paid to verifying the requestor is legitimate. However, this security goal is not relevant for most web-based information providers.

SECURING ELECTRONIC GOVERNMENT
GOVERNMENT AND INDUSTRY PROCUREMENT

Chairs: John Gilligan, CIO, Department of Energy
Guy Copeland, Computer Sciences Corporation

BACKGROUND

Government is capitalizing on the explosion in e-commerce to streamline its procurement processes by buying goods and services using the Internet. By posting opportunities on web-sites, departments and agencies are breaking down barriers to entry and allowing greater access to non-traditional providers. Industry has embraced these changes. Most private sector organizations welcome the opportunity to submit proposals digitally, appreciating the speed and ease of electronic submissions and payments.

In the area of procurement, all five security goals are relevant, and they increase in importance as the value of the procurement increases. For the purposes of this paper, procurements are grouped into three broad size categories, small, medium, and large, with the following characteristics:

- **Small:**
  - Up to $100k
  - Usually using credit cards, purchase orders, etc.
  - No electronic signature required for bid
- **Medium:**
  - Up to $10m
  - Competitive bids (limited): may have a streamlined selection process; may be a schedule purchase; may expect cost / pricing information
  - Time-sensitivity is a factor
- **Large:**
  - Greater than $10m
  - Proprietary information (e.g. technical info responding to procurement)
  - Most potential to include national security information - mixed risk / vulnerability
  - Time-sensitivity is a factor.

Figures for each size are arbitrary and many characteristics overlap, particularly between medium and large. In addition, certain types of procurements may raise problems outside of the size category; this is particularly true if the procurement deals with classified information, or if they include proprietary cost and pricing information. Furthermore, procurements can be categorized by degree of competition. Although sole-source awards remain reasonably common in the national security community, today's environment is inexorably shifting towards competitive procurements. Competitive procurements may be limited, with defined "industry partners" competing

for task orders on a larger government-wide acquisition contract (GWAC), or they may be fully competitive and open to all. As the degree of competition increases, the contractor may need to provide more proprietary or sensitive information to facilitate a department or agency's decision, thereby raising security concerns.

IMPLEMENTING SECURITY

At the most basic level, commercial infrastructures—together with appropriate policies and procedures—provide adequate security for small procurements. However, larger electronic procurements, particularly competitive bids, may require specialized security measures and significant investments to ensure a high level of confidence. This might include improved electronic controls, physical isolation (in some cases), and end-to-end process security for solicitation through closeout and archival.

Availability: As Government relies increasingly on electronic means for soliciting contract support, the demand for reliable availability will increase. At present, the criticality of this service depends on the degree to which alternate means of completing the transaction are in place. For small procurements, priority and time sensitivity is often relatively low, commercial infrastructures such as credit cards are reliable, and paper back-ups are prevalent. In this area, therefore, the cost of unavailability is simply not high enough to warrant special government investment. In contrast, availability is more of a concern for medium and large procurements. These will require redundant systems, specific protections against denial of service attacks, high-reliability equipment, and recovery plans for every contingency. Interestingly, however, the degree of competition does not significantly impact availability as a security goal.

Identification/Authentication: Paralleling availability, challenges in identification and authentication emerge only at the medium and large e-procurement levels. At the small level, identification is handled primarily through credit companies and physical signatures. For mid-size bids, access control and compatibility begin to emerge as challenges. To address these concerns, solutions may range from implementation of digital signature policy and technology through launch of a full-scale public sey infrastructure (PKI). Competition may dictate the solution. Sole-source bidders are already well-known to the procuring department or agency, who most likely possesses data on past technical and financial performance and can use this to identify or authenticate submissions. In a limited competition environment, the department or agency will be familiar with some bidder information (particularly in a GWAC task order situation), but will probably be less able to identify and authenticate data transmissions, requiring a stronger security solution. Finally, fully competitive procurements may draw bidders unfamiliar to the department or agency; therefore, identification and authentication can be completely assured only through a comprehensive solution such as full-scale PKI implementation.

Challenges for identification and authentication at the large procurement level are similar to those at the medium level but the requirement for authentication is even higher. Full PKI with tokens (multi-factor authentication), application-based security,

and hardware solutions will help address the challenge. Large procurements also require appropriately sized solutions and a greater emphasis on internal controls. Choice of these solutions should be dictated in the same manner as with medium-sized procurements.

Confidentiality: At the small procurement level, challenges and solutions for confidentiality mirror those in the above areas: policies and procedures that emphasize good practices such as enabling SSL. At the mid-size procurement level, challenges include securing confidential information such as cost, pricing, proposal information, and privacy. The solutions include some of those listed above, such as strong encryption and host-based controls. Solutions also depend on the type of data; there is a value decision on what level of protection is appropriate. When cost and pricing data is present, much greater care should be taken. When multiple types of data are concerned, security must move to the highest common denominator. The challenges for large procurements are similar, but bigger and tougher since the data includes more potentially sensitive information. Suggested solutions include making large procurement security the standard, though there are concerns about cost and the ability of small companies to play to those constraints. Specific options include implementing appropriate controlled environments (dedicated networks), full VPN, full encryption, strict internal access controls (e.g. read only documents, limited print capability), and full vulnerability and risk assessments.

The degree of competition's impact on confidentiality is less clear than the affect of size. Sole-source and competitive procurements both entail transfer of sensitive performance and financial data, making confidentiality a major security goal.

Integrity: Data integrity must be maintained at all times, especially in competitive procurements. Again, departments and agencies know their sole-source bidders and thus can vouch for the integrity of their data through other means. With limited and fully competitive procurements, the tie that facilitates integrity assessments breaks. A robust combination of host- and application-based controls, which could include dedicated networks and full encryption as well as strict internal access controls, should meet the integrity challenge, regardless of procurement size.

Non-Repudiation: The key driver in this area is the degree to which time sensitivity and/or competition is involved. However, the size of the procurement is probably not a key element. Procurement offices, especially those that deal with competitive bids, should have strong programs to ensure that the sender of the information is provided with proof of delivery and that they are provided with proof of the sender's identity. Without these controls in place, organizations leave themselves exposed if bidders lodge a protest. In the paper-based world, most contractors will ask for a signed receipt—this same functionality is needed in the digital environment.

SECURING ELECTRONIC GOVERNMENT
FINANCIAL TRANSACTIONS TO THE PUBLIC

Chairs: Sky Lesher, Deputy CFO, Department of Interior
Richard Carlson, Novell

BACKGROUND

Financial transactions to the public may have the most far-reaching impact of the e-services considered in terms of number of citizens served. For the purposes of this document, this service is defined as any that allows citizens to apply for or receive financial benefits or information online from Government agencies, such as the Social Security Administration or agencies that provide student loans. This includes transactions where citizens receive the payments in paper form (i.e., a check in the mail) or digitally (a direct deposit into a bank account) after applying online.

One driver for the promulgation of online financial transactions across the Government is the Government Paperwork Elimination Act. This act, passed in 1998, requires agencies to offer their paper-based processes digitally by 2003. The degree to which a department or agency has complied will serve as one of the criteria for judging further information technology budget requests.

A second, equally important, driver is competition from, and best practices developed by, the private sector. Citizens conduct significant financial transactions on line every day—they transfer money between accounts, pay bills, buy stocks, and purchase all manner of goods and services via the Internet. They expect, and are demanding, that Government provide the same type of services. Private sector organizations are also beginning to offer "brokering" services to the public—serving as a "go-between" for users who find it difficult to navigate through the system.

Of the three e-gov services discussed in this paper, financial transactions to the public may present the greatest potential risk to users. Money is an attractive, easy target to would-be thieves. The good news is that industry faces many of the same challenges and has been tackling them for many years. Indeed, the financial services industry is hugely reliant on public confidence. As a result, the Government can often apply commercial standards when implementing technical solutions. However, as demonstrated below, in the areas of policy and implementation, government faces additional challenges.

IMPLEMENTING SECURITY

Whereas security practices in the two previous e-gov services may vary depending on type of information or size of procurement, security requirements for financial transactions remain relatively constant. Each security goal, however, has several layers of complexity.

Availability: In the area of availability, three high level considerations are key. The first is providing access to personal financial records. The Government must provide its services to the entire population. Although computer ownership and use are growing rapidly, large segments of the population do not have easy access to a computer or the skills to conduct on-line transactions. Of course, paper-based processes will remain available for the foreseeable future. However, looking strategically, the Government might consider installing public use kiosks in the lobbies of government buildings. The Veteran's Administration is actually taking laptops out to the field, providing benefits to homeless veterans across Florida.[3]

A second, related consideration, is ensuring the availability of the site and service. The web-based information services section covers many issues related to site availability. Currently, some on-line services are only offered during regular business hours. However, the public is beginning to expect service 24 hours a day, 7 days a week. Further, in the case of failure, regardless of the cause, organizations should have disaster recovery and continuity of operations plans in place—and have practiced them. These plans are significant enablers to the smooth restoration of service.

Finally, Government organizations must maintain interoperability to support financial transaction processing. In general, the private sector tends to be much more nimble in its ability to implement new technology. To the extent that Government must interact with the private sector to deliver this service, departments and agencies will need to ensure systems remain interoperable. In addition, as Government implements its own new systems, it will need to ensure seamless transitions to the new services.

Identification/Authentication: In the area of digital identity, Government will need to meet the standards set by the commercial sector for financial transactions. Financial organizations have a strong motivation to ensure that only authorized users have access to financial data and funds. Technical standards and practices set in the private sector will usually be sufficient for Government organizations.

One area that is unique for the Government, however, is in electronic benefits transfers (EBT). State governments have begun in earnest to use EBT as a cost-effective way of providing benefits to its citizens–from credits for food to cash payments. At the Federal Government level U.S. Department of Agriculture's Food and Nutrition Services is providing food stamps in this way. As more and more programs implement EBT, the need for consolidating the number of cards received by any one person may develop. Even now the Government is beginning to address the issues surrounding a single digital identification card. Among the key questions to be answered are:

- Who would issue it?
- How should the Government balance the needs for physical and digital identification?

---

[3] *See http://www.accessamerica.gov/docs/homelessvan.html*

- How should it address attempts at forgery
- Will the public view this as a threat to their privacy?
- Will digital identity cards become mandatory?
- Will there be a penalty for lost cards?
- How can the Government increase public trust?

Confidentiality: Technical solutions are not exceedingly difficult to assure confidentiality—the challenge is in the policy area. On the technical side, organizations should be able to encrypt data in transit and partition information such that access to the data is on a by-exception basis.

The real challenge is in setting and enforcing the rules that govern who is allowed access to any given piece of data. For example, within the organization perhaps only a small subset of employees is allowed to see all data. Others may have access to a select set of records. These rules apply to users as well; clearly they would have access to their own personal information. In some cases, though, individuals might have access to information on people for whom they have power of attorney; a mother, father, or child, for example.

Of the three e-gov services, the public's dichotomous feelings about Government manifest itself greatest in financial transactions. On the one hand people expect Government to provide benefits—food stamps, Medicare, Social Security, etc. On the other hand, citizens are generally wary of Government holding such private information. Of particular concern is the potential sharing of data between Government organizations. Departments and agencies will have to deal with these issues on a policy, rather than a technical level.

Integrity: Data integrity is also of paramount importance in the financial transactions area. Many citizen's livelihoods and well-being (physical and financial) are dependent upon benefits provided by the Government. If these were somehow compromised, their ability to survive might be at risk.

Data should be protected on two levels—from direct manipulation by an insider or external attacker and from indirect consequences, such as a system error. Susceptibility to external attack can be mitigated through judicious use of techniques such as intrusion detection and firewalls at multiple points in the system. Insider attacks are some of the most difficult to prevent and detect—especially when the attacker is a trusted insider. Technical solutions alone will not address this latter category.

The second way data integrity could be compromised is indirect—through a system error, power outage, or attack somewhere else in the system that has cascading consequences. In these cases, firewalls can help prevent widespread effects. However monitoring software and programs should also be in place. In addition, policies should be implemented and widely disseminated to guide actions in the case of an attack or failure.

Non-repudiation: For their own protection, Government organizations should ensure that mechanisms are in place to confirm the identity of the recipient as well as proof of delivery. Even though the monetary value of the transaction may be relatively small, its worth to the recipient may be very large. For legal purposes it is important to keep records in case any aspect of the registration for or receipt of the benefit is challenged.

CASE STUDIES

The following case studies are drawn from presentations at the May 2000 workshop and explore the differences between three types of e-gov services when considering security goals and solutions. Each case focuses on the link between a specific type of e-gov service, the character of information exchanged, the security priorities and decision factors that the organization considered, and the security solutions it chose. The cases demonstrate that security priorities and solutions vary with the type and characteristics of the e-gov service.

The three case studies validate the general insights and lessons laid out in the main report. The DOE and NASA examples each compare two existing e-gov services to highlight different security concerns and priorities in the same transaction area. For example, the NASA case highlights the differences in security concerns and solutions for two procurement systems: one that handles medium sized procurements and one used for large contracts. SSA's PEBES application is the third case. This study outlines security obstacles that the organization faced a number of years ago when it began to bring financial information to the public online. Although the SSA example is older than the other two, the important lessons-learned about public perceptions and confidence are equally applicable today.

Each case study describes how one organization set security priorities and selected security solutions for a particular type of e-gov service. They are not endorsements of a particular approach, nor do they reproach solutions that the organization did not select. While the studies are excellent illustrations of how security evolves to reflect the particular type of e-gov service, they do not represent endorsed risk management methodologies, certification and accreditation processes, or detailed planning guidance. A multitude of other studies and papers already cover these areas, but few illustrate the importance of considering the type of e-gov service and information content in the security planning process.

GOVERNMENT AND INDUSTRY PROCUREMENT CASE STUDY
NASA ACQUISITION INTERNET SERVICE

SUMMARY

The National Aeronautics and Space Administration (NASA) was among the first government agencies to move procurement into the Internet age. Specifically, the NASA Acquisition Internet Service (NAIS) has launched two e-government initiatives for medium and large procurements. The Request for Quotes System (RFQS) and Electronic Procurement System (EPRO) demonstrate the benefit of tailoring security goals and solutions to specific types of electronic government services—procurement in this case. They also highlight the importance of examining the type and value of information exchanged by e-procurement services when considering security priorities and decisions.

OVERVIEW

NAIS is a grass-roots organization, consisting of functional and technical experts who, largely through consensus building, work to enhance and build e-procurement services. The NAIS goal is to cut paper and reduce bureaucracy in the NASA acquisitions process.

In 1994, just as the Internet emerged as a new communications and business medium, NAIS began to examine electronic means to streamline NASA's procurement process. NASA became the first in the federal government to post all business opportunities over $25k exclusively on the Internet. After much success with the initial foray into electronic commerce, the NAIS team decided to try and close the loop with industry. The results were two bi-directional exchange programs: RFQS and EPRO. These efforts began life as parallel prototypes in 1996 and pilot programs in 1998. Originally each of the programs was geared toward simplified acquisitions ($25,000 - $100,000). In 1998 NAIS selected RFQS as the best option for acquisitions utilizing Simplified Acquisition Procedures (SAP) ($25,000 - $100,000 or commercial items up to $5million), while EPRO was transitioned into a solution for larger procurements. As of late 2000, RFQS is in full service for lower dollar value procurements. EPRO, because of its longer contracts cycle for mid-range and large procurements, remains in the pilot stage.

RFQS and EPRO have a number of similarities and dissimilarities that have affected the way NAIS views and addresses their security goals and solutions:

- RFQS: The Request for Quotes System is an exchange effort for procurement requests of noncommercial items under $100 thousand and commercial items up to $5 million (sums small enough that no contract is necessary). RFQS is based on a mix of commercial-off-the-self (COTS) and tailored solutions and is used by all NASA centers. It is up to the specific contracting officer to decide whether RFQS is the sole method for submitting quotes, or if he or she will also accept fax and paper submissions.

- EPRO: The Electronic Procurement System is a high-range exchange system for procurement requests. It includes noncommercial contracts over $100,000 and commercial items over $5 million. EPRO is based entirely on COTS solutions and, in its present pilot phase, has a limited number of users. However, in procurements where the pilot is used, it is the only means of submitting bids.

SECURITY GOALS

NASA's security goals for its electronic procurement systems are based on mix of the organization's overall goals and requirements and objectives for the RFQS and EPRO systems in particular. NASA has high standards for overall IT security because of the sensitive nature of the Agency's business. The organization spends large sums of money and dedicates much time and attention to cyber security, though funding these efforts is a continuing challenge. Therefore, much of the security for RFQS and EPRO is provided at the corporate level in response to Agency level goals. At the application level, NAIS followed a planned approach to identify security goals during the system design phase. The group identified goals for each system, though it did not prioritize them; they viewed each goal as zero-sum—all goals had to be addressed. After the pilot phase for RFQS (EPRO is still in the pilot phase), NAIS performed an operational readiness review that included additional security inputs from both technical and functional experts.

For RFQS, availability and integrity are crucial system security goals. Confidentiality has also warranted attention, while authentication and non-repudiation are secondary concerns.

- **Availability**: For some business opportunities, RFQS is the only means for vendors to obtain information and submit quotes. Even temporary loss of service could seriously impact business functions. NAIS, therefore, recognized the need to guarantee RQFS availability for all vendors.

- **Integrity**: Because of its large role in the Agency's simplified and commercial items procurements, NAIS emphasized the need to protect data on RQFS from unauthorized modification or destruction. Vendors and contract specialists must be assured that the data on the system is accurate in order to conduct business.

- **Confidentiality**: Though less important at the dollar level associated with RFQS than with large procurements, NAIS recognized that basic protection from eavesdropping is important to assure vendors that their quotes are secure.

- **Authentication and identification**: Authenticating the identity of the vendor placing a quote in RQFS is not as important as ensuring availability and integrity. The system is open to any vendor without registration. Authentication is achieved largely through phone calls to the winner.

- **Non-repudiation**: Since each individual contract specialist using RQFS decides when to cut off quotes for a particular procurement, concerns over non-repudiation were not great – either the quote is in or it is not. Still, some date/time stamp for the contact specialist and a receipt for the vendor is useful.

NAIS determined that EPRO has similar security priorities, but each is amplified because of the size of the procurements in question. EPRO deals with contracts worth billions of dollars, with proposal preparation costing vendors millions of dollars in some cases.

- **Availability**: While availability is important to RQFS, it is even more essential for the EPRO pilot. The pilot is the only avenue to submit bids for those procurements using the application. If EPRO is not available, those bids cannot move forward on schedule.

- **Integrity**: Although integrity is an essential goal for RQFS, it is even more important for the EPRO pilot. If attackers were able to steal or alter data, they could cost vendors and NASA millions of dollars in proprietary information.

- **Confidentiality**: Ensuring that vendor data is not intercepted or observed en-route is a larger concern with EPRO because of the size of the contracts in question and the use of more proprietary information. Again, the loss of proprietary information could be costly to both the vendor and the government.

- **Authentication and identification**: The larger size of EPRO procurements also requires the addition of digital non-repudiation and authentication in the form of electronic signatures. EPRO security goals call for each vendor to be authenticated prior to submitting a bid.

- **Non-repudiation**: Whereas non-repudiation was not a major goal for RFQS, the size and importance of EPRO bids requires a means to validate when a bid was received.

Figure 1. Goal Priority

	RQFS	EPRO
Availability	High	High
Integrity	High	High
Confidentiality	Medium	High
Authentication & Identification	Low-Medium	High
Non-repudiation	Low-Medium	High

In both cases, NAIS found that security requirements and expectations in the electronic environment are considerably higher than those for equivalent functions in the paper world. In the latter environment, for example, a wet ink signature provided the necessary level of security. In comparison, many large electronic procurements demand digital signatures to verify identity.

SECURITY SOLUTIONS

The security solutions NAIS selected for RQFS and EPRO are similar due to overall NASA requirements and their mutual procurement role. The main difference lies in the use of digital signatures for authentication and non-repudiation in EPRO.

Both RQFS and EPRO security rest on NASA's strong network and server protection. This includes firewalls, virtual private networking, secure shells and strong authentication mechanisms, Netscape secure server, and web directory navigation limitations. These and other security mechanisms are in place regardless of the specific e-procurement application. These corporate level measures support data integrity and service availability goals.

Beyond the overall corporate level security, functional experts in the NAIS group decided that it was important for RQFS data to be encrypted in transit with 128 bit secure socket layer to protect vendor information. They also recognized the priority of ensuring that intruders cannot access the RQFS database and modify bids once they are submitted. To do this, NAIS relied on the robust corporate security described above. They also implemented specific policies and procedures to mitigate risks. These included limited access, internal controls, restrictions on remote access, phone verification of quotes, and total restriction on the ability of vendors or other parties to modify quotes after they have been submitted (if the vendor needed to make a change, they have to submit a new quote).

The security solutions for EPRO mirror those for RQFS in many ways, though the scale of the procurements in EPRO has mandated some additional security. EPRO, like RQFS, makes use of encryption and relies on NASA's corporate level security. The encryption takes on added importance because of the increase in vendor proprietary information on EPRO. Unlike RQFS, NAIS decided that the EPRO pilot should use digital signatures for non-repudiation. Because of the size of the contracts in question, the group came to the conclusion that voice verification on its own was inadequate.

Figure 2. Security Solutions

	RQFS	EPRO
Availability	▪ Corporate level security ▪ Firewalls, intrusion detection, VPN, secure shell, authentication mechanisms navigation limitations, etc.	▪ Same
Integrity	▪ Corporate level security ▪ Policies and procedures restricting ability to change data	▪ Same
Confidentiality	▪ Encryption: 128 bit SSL	▪ Same, plus ▪ Digital Signatures
Authentication & Identification	▪ Contract specialists call winner	▪ Digital Signatures: available only to authorized vendors ▪ Contract specialists
Non-repudiation	▪ Contract specialists call winner ▪ Time and date stamps on electronic submissions ▪ Contractors have option to receive return e-mail	▪ Digital Signatures ▪ Time and date stamps ▪ Return Receipt

Even in the pilot phase, EPRO has required more buy-in from other parts of the organization than RQFS. This is primarily due to the addition of digital signatures and electronic forms and the training and education they require. In addition, while RQFS is voluntary and contracting officers may use alternate means, EPRO is mandatory for those using it during the pilot.

As stated before, the NAIS group used grass-roots consensus building to make the vast majority of its security solution choices. The team benefited from a variety of expertise that allowed NAIS to balance security with functionality. In some cases there was a tendency for the functional experts to push for more and stronger security because they felt that the security level in the paper world was not adequate for Internet based applications. In other cases, technical experts advocated more robust security; technical experts wanted to authenticate every user in RQFS, for example, while the functional experts were concerned that this would limit the usefulness of the system. Overall, the team was concerned that adding too much unnecessary security overhead would have a high cost and detract from the benefits of bringing the service online. Hence, functionality generally won when it conflicted with security, though NAIS endeavored to guarantee both. The success of RQFS and EPRO to this point seems to support this approach.

CONCLUSION

The NAIS experience with RQFS and EPRO demonstrates the challenges and opportunities associated with bringing procurement into the electronic, web-based environment. These services are streamlining the government procurement function,

bringing greater ease to users at both ends. However, associated with these benefits, come risks and security concerns—most of which were not present in the paper-based world. Many of the security goals and concerns identified by NAIS are particularly important to the e-procurement function elsewhere in government and industry. The NASA case demonstrates the importance of identifying goals and selecting solutions that are tailored to the type of e-government service and the requirements levied by the nature of the information exchanged.

The NAIS case leads to four lessons-learned that may be applicable to other parts of government and industry procurement:

- The web environment brings new security requirements and expectations to the procurement business. Security experts should address these at the functional and technical levels.
- Different sized procurements—which rely on the exchange of more or less sensitive information—require tailored security solutions. While all e-procurement services focus on availability and integrity, larger procurements require more robust solutions that also address confidentiality, authentication, and non-repudiation.
- It is essential to include functional experts in the security process from day one. Garnering technical and functional input will more likely result in solutions that appropriately balance security and functionality.
- Additional security restraints and requirements should be examined carefully and weighted against their costs.

WEB BASED PUBLIC INFORMATION CASE STUDY
DEPARTMENT OF ENERGY

SUMMARY

The Department of Energy (DOE), like many government and business enterprises, provides a large and varied amount of information to the public. The growth of the Internet has moved this process away from the paper-based medium and into the electronic realm, making distribution easier, but increasing security concerns. Service availability and data integrity are the core security goals for the Department's web-based public information services. DOE addressed these and other security goals with both corporate level and application specific solutions.

OVERVIEW

DOE's web-based information services began, like almost every other organization's, as a decentralized, proactive response to a promising new technology. Web sites resided on the public segment in front of the firewall where they were not adequately protected. Security for web servers and applications was provided by individual "owners," resulting in a wide range security goals, solutions, procedures, and standards. Like many other private and public sector organizations, DOE experienced a very public security incident—its web page was defaced—early in its Internet experience. Although this incident did not cause significant damage, it served as important catalyst for improving security.

DOE's response was to evaluate its network architecture and develop an enterprise-level solution--the screened subnet and centralized administration of key services. The screened subnet is a protected area of the network behind or beside the organization's firewall that is defined as separate network segment. It hosts web servers and applications that can be accessed by the public over the Internet and by users from inside the organization's "private" network. Centralized management facilitates a standardized approach and a robust security posture for DOE's network.

In many instances, the security provided by the subnet is sufficient. In other cases, however, the type of information, or the nature of the interaction with the public demands additional security. To illustrate this point, this case study focuses on two DOE services available to the public--Jobs ONLINE and statistical information.

Jobs ONLINE is the Department's common automated recruitment system that allows applicants to apply for certain DOE jobs over the Internet. Interested applicants can review the vacancy announcement and answer position-specific questions while at this web site. By using Jobs ONLINE, applicants can also choose to receive e-mail notifications of job openings, as well as notification of the status of each job for which they have applied. After the vacancy closes, human resources personnel use the system to automatically rate, rank, and certify candidates. Jobs ONLINE runs on a secure private database and, as of late 2000, is emerging from end-user training.

DOE also uses the Internet to provide a vast quantity of energy data to the public. Types of data range from statistics on fuel stockpile levels, to environmental regulations, to major energy trends. Customers vary from large energy corporations to watchdog groups and individuals. Much of the data is important for the smooth functioning of the energy sector. For example, companies use the information to make business decisions to increase or decrease production of various fuel types. DOE statistics on home heating fuel oil stocks, for instance, are important to companies as they plan production, as well as to government and private organizations who provide fuel relief.

SECURITY GOALS

Overall corporate-level concerns and application-specific security priorities drive DOE's security goals in its web-based information services. Service availability and data integrity are the two security goals that are common to every web-based information service. These common goals were a major driver in the development of the centralized screened subnet solution. As discussed in the main body of this report, the public has high expectations for online Government services. At the same time, the smooth functioning of Government is highly dependent on public confidence. If either availability or integrity is compromised, the effect on the Department may be severe.

For the Jobs ONLINE application availability, integrity, and confidentiality are the most important goals.

- **Availability and Integrity**: The public expects the employment site to be up and running (available) with accurate data (integrity) when they are looking for information. Deficiencies in availability or integrity may cause job seekers to look elsewhere, depleting the pool of qualified candidates and, ultimately, hurting the Department.
- **Confidentiality**: The job-seeking public expects the Department to ensure the security of their personal information. Confidentiality is not as important to many other web-based information services on the screened subnet, because information flows in only one direction: to the public. Jobs ONLINE, in contrast, is a bi-directional exchange. The public views information on job openings and downloads forms, and then submits applications to the Department.
- **Identification, Authentication, and Non-repudiation**: DOE does not need to establish and authenticate an external user's identity until they get further along in the job application process. Inside the Department, however, identification and authentication are important to ensure that unauthorized employees cannot view or alter data.

Security priorities for DOE's web-based statistical information services are also driven by internal and external concerns.

- **Availability and Integrity**: Availability is important in the statistical information area since timely access to energy data may be essential to industry and other consumers. For the same reasons industry and the public expect the posted data to be accurate and reliable.
- **Confidentiality**: Unlike Jobs ONLINE, however, confidentiality is not a major factor for statistical information since most data travels on a one-way street to the public. In most cases, the Department does not take information from the public.
- **Identification, Authentication, and Non-repudiation**: DOE has not found it necessary to identify and authenticate individuals viewing statistical information. However, internally, as with Jobs ONLINE, it is important to ensure that only authorized users can alter posted information. If an unauthorized party altered or destroyed data, the energy sector could suffer.

Figure 1. Goal Priority

	Screened Subnet	Jobs ONLINE	Statistical Info
Availability	High	High	High
Integrity	High	Medium	High
Confidentiality	Med. (some apps)	High	Low
ID & Authentication	Not addressed	Medium (internal)	Medium (internal)
Non-repudiation	Not addressed	Medium (manual)	Low

SECURITY SOLUTIONS

DOE follows a controlled process to develop an implementation plan for each application. Through this process, configuration management committees make security decisions regarding DOE web-based information applications. The key question for security experts is whether or not the application or service needs to be accessible to the public? If the answer is yes, then the application is linked to the secure screened subnet and benefits from that high level of security to guarantee availability and data integrity. Concerns or goals that are not adequately covered by the screened subnet (some access limitations, some policies and procedures, etc.) are the responsibility of the organizations that own the process.

The screened subnet establishes a separate protected network segment behind or beside the firewall. Meanwhile, the information is hosted in a physically secure environment to further ensure integrity. The layered cyber defense makes use of host-based intrusion detection, firewalls, application controls, remote monitoring of availability, manual controls for accounts, in addition to routine vulnerability scanning, auditing, and other tools. Together these provide protection to ensure high availability and security. Department security experts decided that the Jobs ONLINE and statistics applications needed to be both secure and accessible to the public. Once DOE made that decision, it placed both services on the screened subnet where all applications receive robust baseline security. The Department then instituted additional security measures, such as limited access, for Jobs ONLINE and particular statistical information services.

As mentioned above, confidentiality and availability are the two most important goals for the Jobs ONLINE application. Other goals are also addressed, though with less emphasis and often by manual or verbal means. Security solutions for each goal include:

- **Confidentiality**: Since confidentiality is not a major issue when an individual is simply viewing the job offerings, this portion of the process is not encrypted. However, as soon as the application process begins, the session is encrypted end-to-end to ensure that the applicant's personal information may not be viewed by unauthorized third parties. Also, the screened subnet's robust security ensures that unauthorized parties do not view the applicant's information once it resides on DOE's physically secure database. Internally, access controls allow only authorized staff to view applications.
- **Availability**: Availability is provided through the screened subnet. The subnet ensures that outside parties, through denial of service attacks or other means, cannot degrade or destroy the Jobs ONLINE service.
- **Integrity**: This goal is also provided through the screened subnet. The subnet ensures that unauthorized parties cannot change, manipulate, or destroy data. This helps guarantee that the information viewed by the public is in its original, intended form.
- **Non-repudiation**: The application submission process includes a time and date stamp, which human resources can use to establish when an applicant submitted his or her information.
- **Authentication and identification**: There is no electronic authentication for external parties; anyone can apply using Jobs ONLINE. However, once the applicant is offered a position, human resources staff implement the normal procedures for verifying identity and work eligibility. Also, internally, there are access controls to assure that only authorized persons may post or update job listings, or access submitted applications.

Security solutions for DOE's publicly available statistical information are largely provided by the screened subnet because availability and integrity are the chief security goals. Security solutions for each goal include:

- **Integrity**: Data integrity is provided through the screened subnet. The subnet ensures that unauthorized parties cannot change, manipulate, or destroy data. This helps guarantee that the information viewed by the public is in its original, intended form.
- **Availability**: The screened subnet ensures that outside parties, through denial of service attacks or other means, cannot degrade or destroy the statistical information.
- **Confidentiality**: Statistical information travels to the public on a one-way street. Except for special services or applications, consumers do not need to submit any information. Therefore, no particular confidentiality solutions are required for information in transit.

- **Authentication and identification**: Since this information is available to the public, there is no need to establish or authenticate the recipient's identity. However, internally, the Department uses access controls to ensure that unauthorized employees cannot alter data.
- **Non-repudiation**: There is no need to provide proof of delivery for publicly available information.

Figure 2. Security Solutions

	Jobs ONLINE	Web-Based Information
Availability	▪ Screened subnet	▪ Screened subnet
Integrity	▪ Screened subnet ▪ Internal access controls	▪ Screened subnet ▪ Internal access controls
Confidentiality	▪ End-to-end encryption ▪ Internal access controls ▪ Screened subnet	▪ No requirement
Authentication & Identification	▪ Human resources procedures ▪ Internal access controls to view applications or modify	▪ No requirement for access ▪ Internal access controls to modify
Non-repudiation	▪ Time and date stamp	▪ No requirement

Many of the solutions listed above were not required in the paper world, when a smaller amount of information was distributed to the public in hard copy form. The opportunity for intercepting, degrading, or destroying data has vastly increased, requiring these new solutions to guarantee availability and integrity.

CONCLUSION

The DOE experience with Jobs ONLINE and its web-based statistical information demonstrates the challenges and opportunities of providing information to the public online. These services give the public easier access to important information on energy statistics and employment opportunities at DOE. However, associated with these benefits, come risks and security concerns—many of which were not present in the paper-based world. The DOE case demonstrates the importance balancing the need to provide the widest access possible to large amounts of online information, with the associated requirement to ensure security.

The DOE case leads to three lessons-learned that may be applicable to other providers of web-based information to the public:

- Web-based information services face security challenges that were not present in the paper world.
- Availability and integrity are the most important goals for web-based information services to the public. Confidentiality, authentication, and non-repudiation may be

important for particular applications that transfer information both to and from the public.

- Corporate-wide and application-specific measures both have a place in ensuring the security of online information services. It is important to recognize the benefits of institution-wide security, while not ignoring measures, including policies and procedures, which address specific applications.

FINANCIAL TRANSACTIONS TO THE PUBLIC CASE STUDY
SOCIAL SECURITY ADMINISTRATION

SUMMARY

The Social Security Administration (SSA), as the nation's disability and retirement provider, began to exchange financial information online in the mid-1990's. Along the path, however, SSA encountered stumbling blocks with the Personal Earnings and Benefits Estimate Statement (PEBES-now known as the Social Security Statement). Learning from these setbacks, SSA is now pursuing a measured online approach that balances costs and benefits, seeks outside expert input, and ensures wide buy-in from privacy advocates, government leaders, and the public at large.

OVERVIEW

PEBES is the Social Security Administration's definitive report outlining its record of a worker's lifetime earnings and a computation of his or her likely benefits upon retirement. Beginning in 1988, a worker, using his or her name, social security number, and date of birth, could submit a mail or in-person request for a PEBES report. In 1989, SSA began to accept requests for PEBES over the Administration's toll-free "800" number. Regardless of the manner of the request, the PEBES report was sent by mail to the requester at the address he or she provided in the application. By the mid-1990s, millions of workers were requesting PEBES each year. Meanwhile, Congress mandated that SSA send reports to all workers 25 or older by the year 2000. These drivers led SSA to examine on-line methods for the public to request and receive PEBES information.

SSA was among the first federal agencies to go online, launching its web site in May, 1994. Looking to increase public service efficiencies and make the best use of new technology, the Administration began to examine the role the Internet could play in both accepting requests for PEBES reports and in delivering the financial information. In 1994, SSA formed an Electronic Services Delivery Steering Team and partnered with CommerceNet, a public-private Internet consortium, to investigate options. Later, this team would also work with security specialists from Los Alamos National Laboratories to garner additional expert input.

The prospect of placing the PEBES application process and information delivery route online raised a number of important privacy and security concerns, which are outlined in the sections below. The steering team established an incremental approach to address these concerns and bring the PEBES service online. The first phase, which was realized in March 1996 as the Batch PEBES pilot, allowed customers to request the PEBES report online using "shared secrets"—personal identifiers that only the individual and SSA should know-as a way of adequately insuring the customer was who he or she claimed to be. The report was then mailed to the recipient within two weeks. This pilot was so successful that the Administration decided to keep it operational for seven additional months. The second phase, a limited test of the full online request *and* return of the PEBES over the Internet, began in October 1996. After

receiving favorable results, "Online" PEBES began a national test in March 1997. However, within less than a month, a front-page story in *USA Today* brought the effort to a halt. The article claimed that SSA had "inadvertently compromised the financial privacy of tens of millions of Americans" by "trying to speed service and cut costs using the Internet." The article, and much subsequent attention from the media, public, and elected officials, led the Administration to quickly suspend the online service and undertake an extensive review of the problems and issues raised.

SECURITY GOALS

Early on, the steering team recognized that providing adequate security and privacy would be the greatest challenges in bringing PEBES online. However, in the mid-1990's the Internet was so new that simply understanding the security concerns was a major challenge. For instance, encryption was a relatively new concept for SSA security experts because, prior to the Internet, all internal communications were handled over secure lines. Moreover, the mail used to send PEBES reports was no more secure than the glue on an envelope and the threat of prosecution. Why then did the electronic world require so much more security than its paper counterpart? From day one, therefore, security experts had to address not only the "hows" but also the "whys."

One challenge that would prove particularly important a few years later was the public's perception of the Internet and Internet security. On the one hand, the public has continually demanded that the government and private sector provide more and better online services. It clearly recognizes the benefits in ease and time that the Internet lends. However, the public is also far less trusting of the Internet; this was particularly true in the mid-1990's when the technology was extremely new. Individuals have generally expected more robust security online than they would ask for through the mail or via fax. Although SSA was aware of these perceptions when bringing PEBES online, many in the Social Security Administration feel in hindsight that planners paid too little attention to the challenge of managing expectations and securing buy-in.

While the public has set elevated expectations for security on the Internet, it has also tended to hold government to a higher standard than much of the business world. This is particularly true when it comes to personal financial information. This trend may be due to the sensitivity of the information and a perception that government has a special responsibility because the public often has no choice but to provide it with personal information. In any case, because of the sensitivity of the information SSA retains and provides upon request, the public and the media hold the Administration to a particularly high standard.

The SSA team working on PEBES consisted of functional and technical experts. Though it did not follow a formal written process to determine security goals or priorities—none existed in the early going—the team operated within the larger context of SSA and Federal Government regulations and security practices. With the Los Alamos National Laboratory experts, the team concentrated on three major concerns: risk of the

interception of data, risk of penetration to other SSA systems, and authentication to prevent fraud. In the context of the five security goals utilized in the main report, SSA focused on authentication, confidentiality, and integrity.

- **Authentication and identification**: Authentication posed the greatest security challenge for SSA planners bringing PEBES to the Internet. Many of the concerns and risks were the same as in the paper world: concerns that fraudulent requests would result in data being released to unauthorized third parties. The main differences from the paper process were concerns over quantity and visibility. In the online environment, the potential existed for violators to commit nearly instantaneous fraud on a mass scale. In the paper world, by comparison, each case of fraud had to be committed with a separate phone call or mail request. Also, due to the public's attention and security concerns, the Internet raised the possibility that a few incidents of fraud would result in a major reaction against the service.

- **Confidentiality**: The SSA steering team also expressed concern that data sent through the online PEBES service could be observed in transit to the recipient. This was primarily a privacy issue—there was no financial cost to SSA if unauthorized parties viewed a few reports. However, individuals and public confidence could be severely harmed if personal data were subject to interception or observation.

- **Integrity**: Although even "Online" PEBES did not allow the public to alter any data, SSA remained very concerned that the service could act as a gateway for hackers to penetrate the Administration's main data processes. Despite the exceedingly remote likelihood of a successful break-in given the technology used for the PEBES service, the potential cost to the Administration in data and public confidence was extremely high. Therefore, SSA devoted much attention to ensuring data integrity.

- **Non-repudiation and Availability**: SSA determined early on that non-repudiation and availability were less critical priorities for securing the online PEBES service. "Online" PEBES delivered important information to the individual, but it was not essential that this data arrive at a specific, validated time. On the availability side, the consequences of an attack would have proven relatively benign. The greatest damage from a successful denial of service attack would likely be to the Administration's credibility, not to the public's ability to access information. Alternatives such as field offices, the toll-free number, and the mail exist if the online service became unavailable.

Figure 1. Goal Priority

	Batch PEBES Pilot	"Online" PEBES
Availability	Low	Low
Integrity	Medium	High
Confidentiality	Medium	High
Authentication & Identification	High	High
Non-repudiation	Low	Low

SECURITY SOLUTIONS

Prior to moving PEBES online, the SSA steering team addressed major security goals with measured security solutions:

- **Authentication and identification**: Authenticating a user's identity to prevent fraud was the most difficult security challenge. The SSA steering team decided that "Online" PEBES would require the requestor to enter five knowledge-based "shared secrets" to gain access to the information: name, social security number, place of birth, data of birth, and mother's maiden name. This was an improvement over the three identifiers used in the phone and mail request avenues. In addition, SSA posted legal notices informing parties of the penalties of committing fraud. SSA also considered the use of PINS and public key cryptography, but both proved impractical due to cost, number of customers, and frequency of use. Regardless, SSA officials felt that the five questions were proportional security to the value of the data being released.

- **Confidentiality**: To secure PEBES information from interception, SSA utilized the highest level of secure socket layer encryption that was generally supported by web browsers. The steering team felt that this was as good or better security than that provided by the traditional mail method. Additionally, it felt that the value of the information—which, though sensitive, were "not nuclear secrets"—was more than adequately protected in transit at this level.

- **Integrity**: SSA provided data integrity with a robust mixture of firewalls, penetration testing, anomaly detection, and other tools. Specifically, the system was designed such that the public interacted with the firewall secured PEBES server. That server, in turn, interacted with eight mainframe systems behind it that spoke a different language. This system withstood testing by a private third-party "Tiger" team.

As described in the overview, "Online" PEBES was discontinued after increased attention and criticism was leveled against the service. In particular, the privacy community was upset about the five identifiers used in the process. Articles in the press described them as too ubiquitous and portrayed numerous scenarios where a knowledgeable third party could receive the PEBES report. This attention quickly led to increased political scrutiny and a decrease in public confidence. It also led the public to

believe that an intruder could break into the Administration's systems and view, modify, or destroy personal data. Although the potential for this second type of security problem was remote, the perception required SSA to pull all access to the PEBES information off-line.

Today, SSA allows the public to request a PEBES report online, as it did with the Batch PEBES pilot. The information is then sent via the United States Postal Service to the recipient. At the same time, however, the Social Security Administration is moving forward with new online services: an online retirement benefits application process, a retirement planner, and a change of address service for example. For each service, SSA has weighed risk factors to ensure that the new processes do not open up additional vulnerabilities. With the online retirement benefit application, for example, the service only collects information (and only for individuals with direct deposit accounts). This is more efficient than the paper information collection process, but does not open up any new vulnerability. With each new or expanded online application, SSA is also conducting customer surveys, garnering specific input from outside security and privacy experts, conducting consultations with stakeholders, making final consensus decisions to "go live," and rolling out applications gradually to assess security and public opinion.

CONCLUSION

The SSA case leads to six lessons-learned that may be applicable to other providers of financial information and services to the public:

- Personal financial data is a particularly sensitive issue. Though the cost of small-scale fraud may be insignificant to the organization and national well being, it is often extremely important to the individual whose data is in question.
- The Internet environment brings challenges and opportunities to financial transactions that are not readily comparable to the paper world. The public has whole new expectations for security, and holds the government to a particularly high standard.
- Whenever appropriate, organizations should seek input and buy-in from numerous outside sources, including security experts, privacy advocates, and political leaders. An insular approach can often turn out to be counter-productive, even when the security it produces is more than adequate.
- Determining what is "good enough" is not an easy process, though safeguards must be commensurate with the data being protected. Cost/benefit assessments (which also consider non-financial costs/risks) are particularly important when determining the right amount of protection. Moreover, given that no solution is perfect, it is important to talk to as many people as possible to get wide buy-in.
- When possible, organizations should give individuals a choice in whether or not to participate. Letting people opt-out is good, though making them opt-in is even better when the information in question is very sensitive. Though the organization must still guarantee security, individual choice takes away some of the burden of finding the chimerical perfect solution.

- Timing is an important consideration when rolling out new Internet applications. Is the public ready? Congress? The organization itself? Some may argue that the public was not ready for "Online" PEBES in 1996 and 1997—that they would be more willing to have their data online today. Regardless, it is important to bring new services online gradually to assess security and public opinion.